## REMARKS

Claims 1-36, all the claims pending in the application, stand rejected on prior art grounds. Applicants respectfully traverse these objections/rejections based on the following discussion.

### I. The Prior Art Rejections

Claims 1, 4-9, 19, and 22-27 stand rejected under 35 U.S.C. §102(b) as being anticipated by Meyers et al., hereinafter "Meyers" (U.S. Patent No. 5,937,159). Claims 2 and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Meyers in view of Sebes et al., hereinafter "Sebes" (SIGMA: Security for Distribute Object Interoperability Between Trusted and Untrusted Systems). Claims 3 and 21 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Meyers. Claims 10, 12-18, 28, and 30-36 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Meyers in view of Al-Ghosein et al., hereinafter "Al-Ghosein" (U.S. Patent NO. 5,937,159). Claims 11 and 29 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Meyers in view of Al-Ghosein in further view of Sebes. Applicants respectfully traverse these rejections based on the following discussion.

#### A. The 102(b) Rejection Based on Meyers

Applicants respectfully submit that Meyers does not teach or suggest positioning "an untrusted computer between said private computer system and an external computer such that said external computer is prevented from communicating directly with said private computer system . . .wherein only said untrusted application execution contexts of said applications on said untrusted system can communicate directly with said external computer system" as defined by independent claims 1, 9, 17, and 25. To the contrary, as shown in Figure 3 of Myers, the prior art of record only discloses a system and methodology for determining whether users can directly access a computer system and does not disclose the inventive methodology and system that

positions untrusted computer between a private computer system and an external computer. Therefore, once an external computer system has passed the various security procedures described in Meyers, the external computer system is allowed to directly access the trusted or private computer system. To the contrary, in the claimed invention the external computer is prevented from communicating directly with the private computer system.

One major concern is that the external system 12 may try to reach the trusted system 10 to misappropriate data or destroy the trusted system 10. To prevent this, the invention positions an untrusted system 11 between the trusted system 10 and the external system 12. The untrusted system 11 includes an operating system 14 which controls many devices such a storage device 15 (e.g., one or more direct access storage devices DASD). The untrusted system exists to host data or run applications which must be made available to the external network. With the claimed invention the untrusted system includes applications that have trusted application execution contexts 13 and untrusted application execution contexts 16. With the invention, the untrusted application execution contexts 16 cannot initiate communications with the trusted system 16. However, trusted application execution contexts 13 can initiate connections with the trusted system 10. Programs running on trusted system 10 can initiate connections to any context on untrusted system 11.

Thus, if a user on the trusted system 10 attempts to connect to the untrusted system 11 to access some data, the user would be communicating with a trusted application execution context 13 and the connection would be allowed (and data would flow over the connection). However, if an external user 12 (accessing untrusted system 11 via an untrusted application execution context 16) tries to initiate a connection with the trusted system 10, the connection is rejected by the operating system 14. Therefore, the invention allows connections between the trusted system 10 and the untrusted system 11 to be initiated only from the trusted system 10, or from an application running in a trusted execution context 13.

For example, the invention would be very useful where a business has an Internet web page (which would reside on the untrusted system 11) yet still wants to have the Internet web data (in addition to all of its internal business data) accessible by employees who are on the

trusted system 10. In the foregoing situation, the business with the trusted system 10 would need full control over access to the trusted system 10, through conventional security measures (e.g., passwords, physical isolation, etc.).

To the contrary, Figure 3 of Meyers, shows an operating system 304 functionally connected to a plurality of user mode processes through their respective secure boundaries. The ftp SI 301, the login SI 302, the credentials daemon 305 and the A&A Daemon 306 are shown communicating with operating system 304 which isolates each user mode process from all other user mode processes. The A&A is unique because it is also connected the A&A database hardware 307, which implies that all access to the physical storage that holds the A&A data must be made by the A&A Daemon 306 and all other processes are prevented from accessing that storage. Therefore, a user properly clears the secure boundary, is provided direct access to the private computer system. This is directly contrary to the claimed invention that places an untrusted computer between the external computer and the private computer system and prevents the external computer from communicating directly with the private computer system.

In view the foregoing, Applicants respectfully submit that Meyers does not teach or suggest positioning "an untrusted computer between said private computer system and an external computer such that said external computer is prevented from communicating directly with said private computer system . . .wherein only said untrusted application execution contexts of said applications on said untrusted system can communicate directly with said external computer system" as defined by independent claims 1, 9, and 17 and similarly defined by independent claim 25. Therefore, it is Applicants position that independent claims 1, 9, and 25 are patentable over Myers. Further, dependent claims 4-8, 19, 22-24, 26, and 27 are similarly patentable over Myers not only because they depend from a patentable independent claim, but also because of the additional features the dependent claims define. Thus, the Examiner is respectfully requested to reconsider and withdraw this rejection.

**B. The 103(a) Rejection Based on Meyers in view of Sebes**

As shown above, it is Applicants position that Meyers does not teach or suggest positioning "an untrusted computer between said private computer system and an external computer such that said external computer is prevented from communicating directly with said private computer system . . .wherein only said untrusted application execution contexts of said applications on said untrusted system can communicate directly with said external computer system" as defined by independent claims 1, 9, and 17 and similarly defined by independent claim 25. Sebes also does not teach or suggest these features, but instead Sebes similarly allows the external computer direct access to the trusted or private computer ones the external computer has passed the authentication process. For example, in section 3.2 and 3.3, Sebes describes that once an external request has been validated, the gateway allows the external computer direct access to the private or a trusted computer.

Therefore, it is Applicant's position that Sebes similarly does not teach or suggest positioning "an untrusted computer between said private computer system and an external computer such that said external computer is prevented from communicating directly with said private computer system . . .wherein only said untrusted application execution contexts of said applications on said untrusted system can communicate directly with said external computer system." Therefore, no combination of Meyers and Sebes would teach or suggest the invention as defined by independent claims 1, 9, 17, and 25 and it is Applicants position that these independent claims are patentable over any such combination. Further, dependent claims 2 and 20 are similarly patentable, not only by virtue of their dependency from a patentable independent claim, but also by virtue of the additional features of the invention they define. In view the forgoing, the Examiner is respectfully requested to reconsider and withdraw this rejection.

### C. The 103(a) Rejection Based on Meyers

As shown above, it is Applicants position that Meyers does not teach or suggest positioning "an untrusted computer between said private computer system and an external computer such that said external computer is prevented from communicating directly with said private computer system . . .wherein only said untrusted application execution contexts of said applications on said untrusted system can communicate directly with said external computer system" as defined by independent claims 1, 9, and 17 and similarly defined by independent claim 25. Thus, Applicants submit that independent claims 1, 9, 17, and 25 are patentable over the prior art of record. Further, dependent claims 3 and 21 are similarly patentable, not only by virtue of their dependency from a patentable independent claim, but also by virtue of the additional features of the invention they define. In view the forgoing, the Examiner is respectfully requested to reconsider and withdraw this rejection.

### D. The 103(a) Rejection Based on Meyers in view of Al-Ghosein

As shown above, it is Applicants position that Meyers does not teach or suggest positioning "an untrusted computer between said private computer system and an external computer such that said external computer is prevented from communicating directly with said private computer system . . .wherein only said untrusted application execution contexts of said applications on said untrusted system can communicate directly with said external computer system" as defined by independent claims 1, 9, and 17 and similarly defined by independent claim 25. Al-Ghosein also does not teach or suggest these features, but instead Al-Ghosein similarly allows the external computer direct access to the trusted or private computer once the external computer has passed the authentication process.

For example, Al-Ghosein describes a centralized security facility that gives system components a flexible mechanism for implementing security policies. System components such

as applications create a request describing an action that needs to be checked against an appropriate security policy. The request is given to a trust system that determines which policy object applies to the request, and may pass request arguments to the policy. The policy objects include executable code that uses any arguments along with dynamically obtained variable information to make a decision. The decision is returned to the system component, which then operates accordingly. Thus, Al-Ghosein allows the external computer direct access to the trusted or private computer system.

Therefore, it is Applicant's position that Al-Ghosein similarly does not teach or suggest positioning "an untrusted computer between said private computer system and an external computer such that said external computer is prevented from communicating directly with said private computer system . . .wherein only said untrusted application execution contexts of said applications on said untrusted system can communicate directly with said external computer system." Therefore, no combination of Meyers and Sebes would teach or suggest the invention as defined by independent claims 1, 9, 17, and 25 and it is Applicants position that these independent claims are patentable over any such combination. Further, dependent claims 10, 12-16, 18, 28, and 30-36 are similarly patentable, and not only by virtue of their dependency from a patentable independent claim, but also by virtue of the additional features of the invention they define. In view the forgoing, the Examiner is respectfully requested to reconsider and withdraw this rejection.

**E. The 103(a) Rejection Based on Meyers in view of Al-Ghosein and Sebes**

As shown above, it is Applicants position that neither Meyers, Sebes, nor Al-Ghosein teach or suggest positioning "an untrusted computer between said private computer system and an external computer such that said external computer is prevented from communicating directly with said private computer system . . .wherein only said untrusted application execution contexts of said applications on said untrusted system can communicate directly with said external computer system" as defined by independent claims 1, 9, and 17 and similarly defined by

independent claim 25. Thus, Applicants submit that independent claims 1, 9, 17, and 25 are patentable over the prior art of record. Further, dependent claims 11 and 19 are similarly patentable, not only by virtue of their dependency from a patentable independent claim, but also by virtue of the additional features of the invention they define. In view the forgoing, the Examiner is respectfully requested to reconsider and withdraw this rejection.

## II. Formal Matters and Conclusion

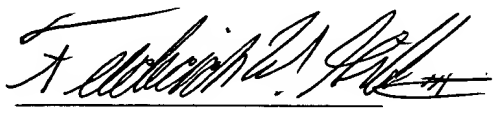
In view of the foregoing, Applicants submit that claims 1-36, all the claims presently pending in the application, are patentably distinct from the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary.

Please charge any deficiencies and credit any overpayments to Attorney's Deposit Account Number 09-0457.

Respectfully submitted,

Dated: 9/7/04



Frederick W. Gibb, III
Reg. No. 37,629

McGinn & Gibb, PLLC
2568-A Riva Road
Suite 304
Annapolis, MD 21401
Customer Number: 29154